

METHOD FOR AUTHENTICATION OF EXTERNAL APPARATUSES IN HOME OR WIRELESS NETWORKS

The invention relates to a method of authentication, particularly in home networks, between a network-internal and a network-external apparatus.

On the consumer market, ease of use is an important sales factor. It includes simple set-up procedures for consumer apparatuses such as televisions, video recorders, etc.

- 5 The best home network configuration would thus be the configuration which is realized by means of automatic procedures without or with only minimal user interaction. Future consumer apparatuses (CE apparatuses) will have a wireless connection. However, the wireless transmission extends beyond home limits and may consequently also be within range of a neighbor's apparatuses. It is thus susceptible to interception and unauthorized
- 10 access. The set-up of a wireless connection therefore comprises two further decisive factors: membership and security. A wireless connection can be established by means of automatic procedures, but an apparatus without any pre-configuration may not be sure that it is connected to the correct network or to a neighbor's network. Moreover, as far as no precautions are taken, the communication can easily be intercepted by a proximate apparatus.

15

- To solve these problems, the apparatuses require a common database with reference to which they can determine whether they belong together, as well as joint security-relevant data such as, for example, a cryptographic key allowing them to protect their
- 20 communication from interception. This joint database must be installed during the configuration process. Conventional methods equip all apparatuses with a user interface for manual entry of the database or offer the user available options, for example, all visible wireless networks, for selection. These methods have considerable drawbacks as far as their ease of use is concerned, because the apparatuses require a corresponding user interface
- 25 (display screen, keyboard, etc.) and the user operation is prone to error, particularly with inexperienced users. To realize a wireless set-up by means of a fully automatic procedure, an automatic procedure solving the membership problem is required. US 2003/0,095,521 A1 discloses a network scheme in which access of short-range network apparatuses to WAN/Internet networks is realized via a kind of "access apparatus" such as, for example,

Handy or PDA having a link with both networks. The authentication between the "access apparatus" and the terminal of the short-range network is realized via a PIN entry. The short-range network may be managed by a third party, for example, a telecommunication provider. In this case, the apparatuses via the user, the seller or the provider are integrated in the network via a PIN pre-registration. This process is performed either via a website or directly via an "access apparatus". The PIN is preferably supplied together with the apparatus.

The known methods have in common that they require user interactions in the form of manual entries, for example, a PIN. Such interactions require corresponding user interfaces and, particularly among inexperienced users, they are prone to error and prove to be inconvenient, particularly for this user group. Moreover, access to the short-range network in the known systems is not spatially defined so that the risk of unauthorized access or interception cannot be excluded.

It is therefore an object of the invention to provide a method of authentication, particularly in home networks, with which a fully automatic integration of wireless apparatuses without any user entry is realized and the risk of unauthorized access or interception is minimized by spatial delimitation.

This object is achieved in that the authentication between a network-internal apparatus and a wireless network-external apparatus is based on a comparison of the values of both apparatuses, which values result from their separate measurements of at least one predefined ambient parameter.

A new apparatus which is to be integrated by means of an automatic procedure in a wireless network first scans the frequency spectrum and establishes a connection with a network-internal apparatus which it has found, for example, an access point. Such a procedure is standardized, for example, in IEEE802.11. This new apparatus must determine whether it is connected to the correct partner (and not to, for example, a neighbor's apparatus), while the network-internal apparatus must determine whether the new apparatus is authorized to be integrated in the network. The invention proposes a solution to this problem which is based on the evaluation of the characteristics of home networks. Two apparatuses check in the following way whether they belong to the same network: one apparatus selects an ambient variable or a set of such variables (such as, for example, temperature, light, etc.) which unambiguously defines the home and, consequently, the home network and transmits these variables to the other apparatus. Subsequently, both apparatuses

perform a measurement of the corresponding ambient values and exchange the results. When the measured values correspond, both apparatuses know that they belong to one and the same network, and the configuration process, in which the network-internal apparatus sends further configuration parameters to the new apparatus, can be continued.

- 5 The object is further achieved by a method, in which the required configuration data are sent from the network-internal apparatus to the wireless network-external apparatus in an encrypted manner and in which the encryption is based on the values of measured, predefined ambient parameters.

- 10 In a further embodiment of the invention, the ambient parameters consist of acoustic and/or optical signals generated by the network-internal apparatus. Defined, time-constant and physically measurable ambient properties are generated thereby, so that deviations between the measured values of the network-external and the network-internal apparatus, caused by measurement time shifts, are excluded.

- 15 Ambient parameters which change upon each request by the network-internal apparatus are defined. It is thereby prevented that an external apparatus repeats the authentication with changing (for example, automatically generated) values until the corresponding values are detected. Alternatively or additionally, the authentication method may be supplemented with further mechanisms so that, for example, after a predefined number of authentication attempts by an external apparatus, further attempts by this
20 apparatus are automatically denied for a given period of time.

- Advantageously, the defined ambient parameters have time-dynamic values. It is thereby prevented that an external apparatus intercepts a successful authentication and retransmits the transmitted data at a later point of time so as to authenticate itself (referred to as "replay attack"). For example, the internal apparatus may itself add defined values or
25 values generated by a random number generator to the communication, which values are transmitted back by the external apparatus in an encrypted form, together with the measured values.

- Following the nature of a home network and the spatial proximity of the apparatuses connected to this network, the invention is based on the principle that the values
30 measurable in the ambience of the network are equal for all participating apparatuses at the instant when the apparatuses are to be configured automatically. However, these values are not detectable by apparatuses outside the considered ambience, i.e. outside the home.

 Further embodiments of the invention are defined in the dependent claims.

These and other aspects of the invention are apparent from and will be elucidated with reference to the embodiments described hereinafter.

5

In the drawings:

Fig. 1 shows the arrangement of a home network;

Fig. 2 shows the flow chart of the method according to the invention, with value comparison, and

10

Fig. 3 shows the flow chart of the method according to the invention, with ambient value encryption.

15

In the example shown in Fig. 1, a home network 1 is arranged with internal apparatuses 21, 22, 23, 24, 25 to which a network-external notebook 3 requests access. After the notebook 3 has performed a scan of available wireless networks, it establishes, for a network authentication, a connection as shown in Fig. 2 with the network-internal access point 21 which is a member of the selected network 1. The access point 21 sends the ambient parameters "temperature" and "acoustic frequency" to the notebook 3. Subsequently, the access point 21 generates an acoustic signal at the frequency F_A . The network-internal access point 21 as well as the network-external notebook 3 now measures the ambient parameters "temperature" and "acoustic frequency", with the latter measurement on the part of the access point 21 being canceled because this frequency was generated by the access point 21 itself. After the notebook 3 has passed on its measured values T_N , F_N to the access point 21, it compares the obtained values with the self-determined values. When the transmitted values T_N , F_N correspond to the own values T_A , F_A , the access point 21 sends the required configuration data to the notebook 3 which performs the corresponding configuration and subsequently connects it to the network 1. When the values passed on by the notebook 3 to the access point 21 do not correspond to the own values, the notebook 3 is denied access to the network 1. In this case, the notebook 3 repeats this procedure with an apparatus of another available network.

25
30

However, this method still does not provide adequate protection from interception. The state of the art offers different methods of securing the communication between the apparatuses. To this end, the network-internal apparatus (access point 21) encrypts the connection with the network-external apparatus (notebook 3) by means of

known encoding methods which are based on modern mathematical methods and provide the possibility of transmitting the required keys via the unprotected wireless interface. Such a method is, for example, the symmetrical Hellman encryption in which each apparatus exchanges half of its key, or the asymmetric private/public encryption principle in which the apparatuses exchange their public keys. The required keys are suitably exchanged before sending the ambient parameters from the network-internal apparatus (access point 21) to the network-external apparatus (notebook 3).

In the method shown in Fig. 3, there is no comparison of the values measured by notebook 3 with the values of the access point 21. The access point 21 directly sends the required configuration data to the notebook 3, which data are, however, encoded on the basis of the determined values "temperature T_A " and "acoustic frequency F_A ". If the ambient values T_N , F_N passed on by notebook 3 correspond to those of the access point 21, the transmitted configuration data can be decrypted and the connection with the network 1 can be subsequently established. If, in the opposite case, the transmitted configuration data cannot be decrypted by the notebook 3, no connection can be established with the network 1.

The proposed methods represent a new paradigm for authentication of a new apparatus in an existing home network, which is based on the interaction between the apparatuses and their ambience. Security-relevant data are the measured results of some defined ambient variables which are determined separately by the new apparatus which is to be configured, and one of the apparatuses already registered in the network. The apparatus which has already been registered serves as the authenticator in this case.

Suitable ambient variables for authentication are, for example, also the acoustic signature of the space or a "fingerprint" of the instantaneous acoustic ambience (such as, for example, an operating air-conditioning apparatus or currently playing music). Alternatively, an ultrasound signal can be generated by the network-internal apparatus. Further suitable parameters are

- modulated light signals (visible or infrared)
- air temperature
- humidity
- light intensity of the ambience
- a (possibly weighted) mixture of a plurality of parameters.

In this respect it is to be noted that the simultaneous measurements by the network-external apparatus to be configured and the network-internal apparatus counteracts faults in the home network, which may be caused by temporal changes of the ambience.

The use of common ambient characteristics is also possible for authenticating apparatuses in power line communication networks which are also vulnerable to interception and unauthorized access because of their internal connections. Furthermore, the use of these characteristics is also suitable for arranging a home network between two apparatuses. In this case, one apparatus is to be assigned the role of the "network-internal" apparatus and the other the role of the "network-external" apparatus. Guest access is also possible. Moreover, the proposed method is also applicable in ad hoc networks which are formed, for example, between arbitrary apparatuses without any access to infrastructure and without pre-exchanged keys. In any case, it should be ensured that unauthorized apparatuses that are present in the same ambience cannot perform the ambient parameter procedure for authentication.

LIST OF REFERENCE NUMERALS:

- | | |
|-----------------|-------------------------------------|
| 1 | network |
| 2 | network-internal apparatus |
| 3 | network-external apparatus |
| 21 to 25 | network-internal apparatuses |